PTO/SB/21 (08-00)
Approved for use through 10/31/02. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMENRCE
Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays avalid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

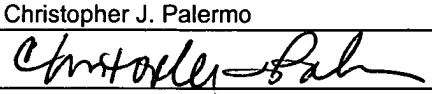
Application Number	09/767,284
Filing Date	01/22/2001
First Named Inventor	Eliot Lear
Group Art Unit	2135
Examiner Name	Klimach, Paula W.
Total Number of Pages in This Submission including this page, check and postcard: 18	Attorney Docket Number: 50325-0517

ENCLOSURES ***(check all that apply)***

- [X] Check in the amount of $500.00 for Appeal Brief Fee
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Assignment Papers *(for an Application)*
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition To Convert To a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, number of CD(s)_____
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [X] Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- [ ] Proprietary Information
- [ ] Status Letter
- [X] Other Enclosure(s) *(please identify below):*
  - Acknowledgment of Receipt postcard

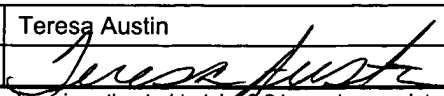
Remarks: The Commissioner is authorized to charge any additional fees, including any required extension of time fees, and credit all overpayments to deposit account 50-1302.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Hickman Palermo Truong & Becker LLP Christopher J. Palermo
Signature	
Date	January 6, 2006

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class: mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this date: January 6, 2006

Type or printed name	Teresa Austin		
Signature		Date	January 6, 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Confirmation No.: 2045

Eliot Lear, et al. Group Art Unit No.: 2135

Serial No.: 09/767,284 Examiner: Klimach, Paula W

Filed on: 01/22/2001

For: METHOD AND APPARATUS FOR SELECTIVELY ENFORCING NETWORK SECURITY POLICIES USING GROUP IDENTIFIERS

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed on October 12, 2005, and in reply to the Notice of Panel Decision from Pre-Appeal Brief Review mailed December 8, 2005, which reset the due date for this Appeal Brief to January 8, 2006.

I. REAL PARTY IN INTEREST

Cisco Systems, Inc. (Nasdaq: CSCO), and its wholly-owned subsidiary Cisco Technologies, Inc., both of San Jose, California, are the real parties in interest.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: **Mail Stop Appeal Brief – Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on January 6, 2006 by Teresa Austin

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-6 and 13-24 are pending in this application, were finally rejected, and are the subject of this appeal. Claims 7-12 were canceled during prosecution.

IV. STATUS OF AMENDMENTS

No amendments were filed after the final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application contains independent Claims 1, 13, 19, 20, 23, and 24. Claims 1, 23, and 24 are method claims. Claim 13 is a computer-readable medium claim. Claims 19-20 are apparatus claims. These independent claims generally recite similar features.

The independent claims generally recite an approach for selectively enforcing a security policy in a network without having to update the security policy whenever a new user enters a network. In one such approach, computer-implemented steps provide for receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists. The definitions include network addresses for the users. The network addresses have been assigned by an address server. One or more access controls are created in a policy enforcement point device that controls access of clients to the network. Each of the access controls specifies that a named abstract group is allowed access to a particular resource.

At some point thereafter, a new user enters the network. The method receives, from an external binding process separate from the address server, a binding of a network address to an

authenticated user of one of the clients for which the policy enforcement point controls access to the network. The named group is updated to include the bound network address of the authenticated user at the policy enforcement point. The method then permits a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

A benefit of the method is that a network administrator does not need to update access control lists or other security measures as users enter and leave a network. Instead, a user's membership in a group binds that user to a particular security policy whenever the user enters the network.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-6 and 13-24 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Reid et al*, U.S. Pat. No. 6,182,226 (hereinafter "*Reid*") in view of *Ray et al*, U.S. Pat. No. 6,587,455 (hereinafter "*Ray*").

Claims 21 and 22 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Reid et al.* in view of *Ray et al.*, and additionally in view of *Stewart* and *Stevens*, respectively.

VII. ARGUMENTS

A. Introduction

To establish obviousness under 35 U.S.C. § 103(a), the references cited and relied upon must teach or suggest all the claim limitations. In addition, a sufficient factual basis to support the obviousness rejection must be proffered. *In re Freed*, 165 USPQ 570 (CCPA 1970); *In re Warner*, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 148 USPQ 721 (CCPA 1966).

Reid and *Ray et al.*, considered alone or in combination, do not teach or suggest all the limitations of Claims 1-6 and 13-24. Further, the Office has not proffered a sufficient factual basis to support the rejection of Claims1-6 and 13-24 under 35 U.S.C. § 103 as being unpatentable over *Reid* in view of *Ray et al.*

B. Claims 1-6, 13-20 and 23-24

Claims 1-6, 13-20 and 23-24 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Reid et al*, U.S. Pat. No. 6,182,226 (hereinafter "*Reid*") in view of *Ray et al*, U.S. Pat. No. 6,587,455 (hereinafter "*Ray*"). The rejection is respectfully traversed. The claims are patentable for at least the reasons provided hereinafter.

INDEPENDENT CLAIMS 1, 13, 19, 20, 23, AND 24

First, each of the independent claims recites receiving information both from **an address server** and from **an external binding process separate from the address server**; however, the references fail to show both such information sources, alone or in the claimed combination. Each of the independent claims 1, 13, 19, 20, 23 and 24 recites a combination that includes:

> **receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;**
>
> receiving, from an external binding process separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;
>
> updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and
>
> permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named

group identified in one of the access controls that specifies that the named group is allowed access to the network

The cited references, alone or in combination, lack at least the emphasized features. Regarding claim 1, for the binding feature, the Office Action recognizes (p. 3) that *Reid* fails to teach receiving a binding of a network address to an authenticated user from an external binding process. To fill this gap, the Office Action proposes a broad definition of "binding" and then contends that *Ray*'s address allocation is the same as the claimed binding.

This is incorrect on several grounds. The Office Action states that applicant does not define binding a network address to an authenticated user, and then defines binding as "imposing an obligation." While the Office Action fails to provide any source of the suggested definition, "imposing an obligation" is a legal definition, not a technical definition, and is not relevant to the subject matter of the invention. "A technical term used in a patent document is interpreted as having the meaning that it would be given by persons experienced in the field of the invention..." *Hoechst Celanese Corp. v. BP Chems. Ltd.*, 78 F.3d 1575, 1578, 38 USPQ 1126, 1129 (Fed. Cir. 1996). The Office Action errs in adopting a legal definition wholly irrelevant to the technical context of binding a network address to an authenticated user.

An appropriate technical definition given Applicant's art for binding is "to make an association between two or more programming objects or value items for some scope of time and place." See WhatIS.com, http://whatis.techtarget.com/definition/0,,sid9_gci211662,00.html. *See also* J. Saltzer, "On the Naming and Binding of Network Destinations," IETF Network Working Group, Request for Comments: 1498, August 1993; J. Saltzer, "Naming and Binding of Objects," 60 Lecture Notes in Computer Science at 99 (Springer-Verlag, 1978) (copies previously submitted during prosecution).

When a correct technical definition is adopted, the address server disclosed by *Ray* cannot correspond to the claimed external binding service. *Ray* teaches a DHCP server as an address server. Applicants teach *both* a DHCP server for address allocation (FIG. 1A, DHCP server 134) *and* a separate NABR server for providing user-address bindings (FIG. 1A, NABR

server 130). Applicant's specification also highlights the differences in function of these elements. Specification, Page 11 lines 20-26 states, "Edge device 122 is communicatively coupled to a Network Address Binding Resolution (NABR) server 130, User Registration Tool (URT) server 132, and Dynamic Host Configuration Protocol (DHCP) server 134. NABR server 130 is responsible for carrying out network address binding resolution to bind an authenticated user of a workstation, e.g., workstation 118, to a particular static network address such as an IP address. ... DHCP server 134 is responsible for dynamically assigning network addresses to devices associated with authenticated end users, e.g., for workstation 118." Therefore, contending that *Ray*'s DHCP server correlates to the claimed external binding service is not logically consistent with Applicant's disclosure.

The DHCP server of *Ray* is not an external binding service. The external binding service persistently associates or maps an authenticated user to a particular static network address. In contrast, DHCP merely assigns IP addresses in response to requests of DHCP clients, but does not perform any binding or mapping. As a result, one of ordinary skill in the art would not correlate the DHCP server recited in *Reid* or *Ray* to an external binding service as claimed, or to an NABR server that performs the external binding process in applicant's embodiment.

Still further, the reliance of the Office Action on particular parts of *Ray* is misplaced. The Office Action asserts that the steps of "receiving, from an external binding process, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network; updating the named group to include the bound network address of the authenticated user at the policy enforcement point;" is expressly described in *Ray* (Col. 4, line 65 to col. 5, line 31). This is incorrect. The text cited in *Ray* for "receiving...a binding of a network address to an authenticated user" simply describes a method for a device to receive a network address from a network server when the device is added to a network (Col. 4, line 65 to col. 5, line 31). *Ray* makes no mention of "an authenticated user," or anything relating to authentication, as featured in Claim 1. Further, receiving a binding of an authenticated user to a network address is not the same as a network address alone. *Ray* has no

teaching of associating, mapping or binding an authenticated user to a network address, or communicating such a binding from one place to another.

Since neither *Reid* nor *Ray* either alone or in combination teach to suggest the use of an external binding service, separate but in combination with an address server as claimed, the rejection is unsupported in the references.

Next, for the claimed feature of "updating the named group to include the bound network address of the authenticated user at the policy enforcement point," the Office Action states that "the firewall saves the network address and therefore updates the group to include the new IP address." However, updating of a group is significantly different than saving a network address. The portion of *Ray* on which the Office Action relies merely teaches saving a network address received from a network device. There is no teaching or suggestion to add the network address to a named group. There is no suggestion to combine the address save operation of *Ray* with any other feature or function at all.

One benefit of the independent claims is to update a group definition only after receiving a binding that associates a network address with an authenticated user. *Ray* has no such suggestion. *Ray* in combination with *Reid* would merely provide for saving a network address as part of a region definition. But such a combination of references fails to provide the complete claimed combination, which performs the update only after receiving a binding of an address to an authenticated user. A combination of the cited references fails to provide the security offered by the claimed approach.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art." *In Re Royka*, 180 USPQ 580; MPEP § 2143.03. However, the cited prior art does not teach or suggest the foregoing features of each of the independent claims. Therefore, the Office Action has failed to present a prima facie case under 35 U.S.C. 103, and the rejection of Claim 1, 13, 19, 20, 23, and 24 is unsupported. Reconsideration is respectfully requested.

CLAIMS 2-12 AND 13-18

Claims 7-12 were canceled in prosecution, so that the rejection thereof is moot. Claims 2-6 all depend from Claim 1 and include all of the features of Claim 1. Therefore, Claims 2-6 are patentable over *Reid* and *Ray* for at least the reasons set forth herein with respect to Claim 1.

Furthermore, Claims 2-6 recite additional features that independently render them patentable over *Reid* and *Ray*. For example, Claim 5 recites "wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a network address binding resolution (NABR) process." Nothing in *Reid* or *Ray* recites the use of a NABR process for the binding process described in Claim 1. The Office Action contends at page 11 that this feature is shown in *Ray* col. 6, line 66 to col. 7, line 7. This is incorrect. *Ray* has no such disclosure. The terms "network address binding resolution" and "NABR" do not appear in the cited passage. *Ray* has no equivalent structure, either, and the Office Action gives no rationale why any other structure in *Ray* corresponds to the claimed NABR process.

As another example, Claim 6 recites determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network. The Office Action refers to *Reid* col. 15, lines 29-49, but this passage does not teach deleting a bound address from a region in response to determining that a user has discontinued using a client. This difference is fundamental. For this reason, the rejection of Claim 6 must be withdrawn.

Claims 13-18 include limitations similar to Claims 1-6, except in the context of computer-readable media. Therefore, Claims 13-18 are patentable over *Reid* and *Ray* for at least the reasons set forth herein with respect to Claims 1-6.

C. <u>Claims 21 and 22</u>

Stewart and *Stevens* are cited to show the ASAP protocol and the DNS process, respectively, with regard to Claims 21 and 22. However, neither *Stewart* nor *Stevens* teach using

ASAP or DNS for receiving a **binding** of a network address to **an authenticated user**, when the term "binding" is properly defined and construed as described above.

Further, Claims 21 and 22 each depend from an independent claim that has the features identified above as distinct from *Reid* and *Ray*. Neither *Stewart* nor *Stevens* cures these deficiencies of the base references. Therefore, a combination of *Stewart* or *Stevens* with *Reid* and *Ray* cannot provide the complete combination that is claimed.

VII. CONCLUSION AND PRAYER FOR RELIEF

Based on the foregoing, the rejection of Claims 1-6 and 13-23 under 35 U.S.C. § 103 as allegedly unpatentable over *Reid* in view of *Ray et al.* lacks the requisite factual and legal bases. Appellants therefore respectfully request that the Board reverse the rejection of Claims 1-6 and 13-23.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Christopher J. Palermo
Reg. No. 42,056

Dated: January 6, 2006

2055 Gateway Place Suite 550
San Jose, CA 95110-1093
Tel: (408) 414-1080 ext. 202
Fax: (408) 414-1076

CLAIMS APPENDIX

1. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving, from an external binding process separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

2. A method as recited in Claim 1, wherein the steps of creating and storing one or more access controls in a policy enforcement point that controls access to the network comprise the steps of:

creating and storing one or more definitions of groups in a data store;

creating and storing one or more definitions of resources within a data store;

creating and storing one or more access controls at the policy enforcement point, wherein each of the access controls specifies that a named group is allowed access to a particular resource, and wherein one of the access controls specifies that all other traffic is denied access to the network.

3. A method as recited in Claim 1, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

4. A method as recited in Claim 1, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user.

5. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a network address binding resolution (NABR) process.

6. A method as recited in Claim 1, further comprising the steps of determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.

13. A computer-readable medium carrying one or more sequences of instructions for selectively enforcing a security policy in a network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving, from an external binding process separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

14. A computer-readable medium as recited in Claim 13, wherein the instructions for carrying out the steps of creating and storing one or more access controls in a policy enforcement point that controls access to the network comprise instructions for carrying out the steps of:

creating and storing one or more definitions of groups in a data store;

creating and storing one or more definitions of resources within a data store;

creating and storing one or more access controls at the policy enforcement point, wherein each of the access controls specifies that a named group is allowed access to a particular resource, and wherein one of the access controls specifies that all other traffic is denied access to the network.

15. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

16. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the network address of the authenticated user and

information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user.

17. A computer-readable medium as recited in Claim 13, wherein the instructions for carrying out the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprise instructions for carrying out the steps of performing network address binding resolution for the user.

18. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.

19. An apparatus for selectively enforcing a security policy in a network, comprising:

means for receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;

means for creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

means for receiving, from an external binding process separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

means for updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

means for permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the

named group identified in one of the access controls that specifies that the named group is allowed access to the network.

20. An apparatus for selectively enforcing a security policy in a network, comprising:
a network interface that is coupled to the data network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;
creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;
receiving, from an external binding process separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;
updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and
permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

21. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from an ASAP protocol process.

22. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a DNS process.

23. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;

creating and storing one or more access control list entries in a network router that acts as a policy enforcement point device and that controls access of clients to the network, wherein each of the access control list entries specifies that a named group of users is allowed or refused access to a particular network resource;

creating and storing one or more definitions of the named groups in a data store that is accessible by the network router;

receiving, from an external process that can bind a user to a specific network address and that is separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the router controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the bound network address to pass from the policy enforcement point into the network only if the bound network address is in the named group identified in one of the access control list entries that specifies that the named group is allowed access to the network.

24. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

receiving information defining one or more group lists, resource definitions, and definitions of users as members of one or more groups in the group lists, wherein the definitions include network addresses for the users, wherein the network addresses have been assigned by an address server;

creating and storing one or more access control list entries in a network router that acts as a policy enforcement point device and that controls access of clients to the network, wherein each of the access control list entries specifies that a named group of users is allowed or refused access to a particular network resource;

creating and storing one or more definitions of the named groups in a data store that is accessible by the network router;

receiving, from an external process that can bind a user to a specific network address and that is separate from the address server, a binding of a network address to an authenticated user of one of the clients for which the router controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point;

permitting a packet flow originating from the bound network address to pass from the policy enforcement point into the network only if the bound network address is in the named group identified in one of the access control list entries that specifies that the named group is allowed access to the network; and

distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user;

determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.